REMARKS

Claims 1-33 and 48 are pending in this application. Claims 1 and 17 have been amended. Claims 34-47 have been cancelled and new claim 48 has been added.

I. 35 U.S.C. § 103(a) Rejection (Claims 1, 3, 5-8, 13-14, 17, 21-22, 24, 27-29, 34, 38, and 41-44)

Claims 1, 3, 5-8, 13-14, 17, 21-22, 24, 27-29, 34, 38, and 41-44 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Nessett et al. (5,968,176) in view of Segal (US 6,345,299).

Claim 1 has been amended to recite

> 1. (Currently Amended) A secure network configured to carry data, comprising:
> a plurality of network bubbles, each network bubble having a plurality of bubble partitions,
> each bubble partition having at least one network device configured to transmit and receive data, and
> all of the network devices corresponding to the same respective network bubble having ~~at least one of the plurality of network bubbles have~~ unrestricted network access with each other and the same network security policy; and
> a network control point having one or more network control point devices, a first network device of a first bubble being connected to the network control point through at least one network control point device and a second network device of a second bubble being connected to the network control point through at least one network control point device wherein the network control point applies the security policy of the first bubble to data for the first network device and the security policy of the second bubble to data for the second network device.

All the devices with the same bubble have the same network security policy. A network control point applies the policy of the respective bubble to data for a device depending on with which bubble the device is associated.

Claim 1 is patentable over Nessett in view of Segal because the combination fails to disclose, teach, suggest or motivate one of ordinary skill in the art to make the invention of claim

1 including a "network control point [which] applies the security policy of the first bubble to data for the first network device and the security policy of the second bubble to data for the second network device." In each of the references, a centralized network security policy is applied to all devices in the network. For example, see Nessett at column 3, lines, 15-57 which describe implementing a "pervasive, multilayer firewall." The firewall implements one security policy. The layers of the multilayer are the different network layers. Different network layer devices perform functions at their appropriate network layer, but they all implement the same security policy across the network.

Accordingly, it is desirable to implement a system which allows for a coordinated security policy implementation across multiple layers of network systems.

SUMMARY

The present invention provides a system for providing security in a network that includes nodes operating in multiple protocol layers and having security functions. Multiple network devices, such as routers, remote access equipment, switches, repeaters and network cards, and end system processes having security functions are configured to contribute to implementation of distributed firewall functions in the network. ***By distributing firewall functionality of the network in a variety of network devices and end systems, a pervasive firewall is implemented.*** The pervasive, multilayer firewall includes a policy definition component that accepts policy data that defines how the firewall should behave. The policy definition component can be a centralized component, or a component that is distributed over the network. The multilayer firewall also includes a collection of network devices that are used to enforce the defined policy. The security functions operating in this collection of network devices across multiple protocol layers are coordinated by the policy definition component so that particular devices enforce that part of the policy pertinent to their part of the network.

For example, a router in the network enforces that part of ***the policy*** that is pertinent to those systems and network devices whose traffic might traverse the router. A switch enforces that part of ***the policy*** that is pertinent to those systems and network devices whose traffic traverses the switch. A repeater enforces that part of the policy that is pertinent to those systems and network devices whose traffic traverses the repeater. A network interface card enforces that part of ***the policy*** that is pertinent to the system or device to which it is connected. In

addition, other parts of the network are included in the multilayer firewall, such as end system operating systems and applications, remote access equipment network management systems for controlling network traffic and monitoring network traffic, and other auxiliary systems such as name services and file services included in the collection of network devices at which the pervasive, multilayer firewall of the present invention is implemented.

Segal discusses sharing the load across firewalls in a network, but the firewalls enforce the same security policy across the network. (See column 2, lines 50 column 3, line 15.)

The network control point of claim 1 enforces different security policies for the different bubbles. Thus claim 1 is patentable over Nessett in view of Segal.

Claim 17 has been amended to recite:

> a network control point having one or more network control point devices, a first network device of the first network bubble being connected to the network control point to which a second network device of the second bubble is also connected wherein the network control point device applies the distinct security policy of the first bubble to data for the first network device and the distinct security policy of the second bubble to data for the second network device.

The arguments presented for claim 1 are applicable to claim 17 as well for demonstrating that it also is patentable over Nessett in view of Segal.

Additionally, the arguments for claims 1 and 17 are applicable for demonstrating that dependent claims 3, 5-8, 13-14 and 21-22, 24, 27-29, and new claim 48 are patentable over Nessett in view of Segal. Claims 34, 38, and 41-44 have been cancelled.

II. 35 U.S.C. § 103(a) Rejection (Claims 2, 4, 10, 23, 25, 30, 33, and 35-36)

Claims 2, 4, 10, 23, 25, 30, 33, and 35-36 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Nessett et al. (5,968,176) in view of Segal (US 6,345,299) and further in view of Williams (6,304, 973).

Williams does not cure the deficiency of Nessett in view of Segal for disclosing or suggesting or the elements of these dependent claims of claim 1 and 17. Therefore, claims 2, 4, 10, 23, 25, 30, and 33 are patentable over Nessett in view of Segal and further in view of Williams. Claims 35-36 were cancelled.

III. 35 U.S.C. § 103(a) Rejection (Claims 9, 11-12, 15-16, 18-20, 26, 31-32, 37, 39-40 and 45-47)

Claims 9, 11-12, 15-16, 18-20, 26, 31-32, 37, 39-40 and 45-47 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Nessett et al. (5,968,176) in view of Segal (US 6,345,299) and further in view of Wesinger, Jr. et al. (6,052,788).

Wesinger does not cure the deficiency of Nessett in view of Segal for disclosing or suggesting or the elements of these dependent claims of claim 1 and 17. Therefore, claims 9, 11-12, 15-16, 18-20, 26, and 31-32 are patentable over Nessett in view of Segal and further in view of Wesinger. Claims 37, 39-40 and 45-47 were cancelled.

Conclusion

In light of the amendments presented above, pending claims 1-33 and 48 as amended are in condition for allowance, and applicant respectfully requests a notice of allowance.

Date: 8/24/06

Respectfully Submitted on Behalf of Applicants

Brian Jemes et al.

Eileen Lehmann

Eileen Lehmann
Registration No. 39,272
Hewlett-Packard Company
Mail Stop 1197
1501 Page Mill Road
Palo Alto, CA 94304
650-857-7940 (telephone)
650-852-8063 (fax)